Strategy Research Project

COMMANDER'S "RIGHT TO KNOW" HEALTH INFORMATION: A STRATEGICALLY FLAWED INNOVATION

BY

COLONEL MICHAEL J. BENJAMIN
United States Army

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
21-03-2011	Strategy Research Project	

4. TITLE AND SUBTITLE

Commander's "Right to Know" Health Information: A Strategically Flawed Innovation

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Michael J. Benjamin

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Colonel Kenneth Lassus
Department of National Security and Strategy

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The military's greatest strategic asset is its personnel. Key to individual quality of life and unit performance is the relationship between service members (SM) and their leaders. Leaders need to know as much as possible about their troops. Meanwhile SMs often want to keep medical information private. Privacy between patients and healthcare providers advances important societal objectives. Compelling reasons justify privacy, particularly in a military context where the negative stigma of seeking behavioral health services is acute. Examining the perspectives of several stakeholders, this paper addresses the strategic implications of the tension between a leader's interest in gathering his subordinates' personal information and the subordinate's interest in privacy. This paper asserts that current Army and DOD guidance is strategically flawed. Current policy risks eviscerating medical privacy and confidentiality and will undermine not only a soldier's quality of life, but also, mission readiness. The paper recommends changing the current guidance to better comport with strategic objectives.

15. SUBJECT TERMS

HIPAA, Health Services and Fitness, Leadership, Confidentiality, Mental Health

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	50	

USAWC STRATEGY RESEARCH PROJECT

COMMANDER'S "RIGHT TO KNOW" HEALTH INFORMATION: A STRATEGICALLY FLAWED INNOVATION

by

Colonel Michael J. Benjamin
United States Army

Colonel Kenneth Lassus
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Michael J. Benjamin

TITLE: Commander's "Right to Know" Health Information: A Strategically Flawed Innovation

FORMAT: Strategy Research Project

DATE: 21 March 2011 WORD COUNT: 7,716 PAGES: 50

KEY TERMS: HIPAA, Health Services and Fitness, Leadership, Confidentiality, Mental Health

CLASSIFICATION: Unclassified

The military's greatest strategic asset is its personnel. Key to individual quality of life and unit performance is the relationship between service members (SM) and their leaders. Leaders need to know as much as possible about their troops. Meanwhile SMs often want to keep medical information private. Privacy between patients and healthcare providers advances important societal objectives. Compelling reasons justify privacy, particularly in a military context where the negative stigma of seeking behavioral health services is acute. Examining the perspectives of several stakeholders, this paper addresses the strategic implications of the tension between a leader's interest in gathering his subordinates' personal information and the subordinate's interest in privacy. This paper asserts that current Army and DOD guidance is strategically flawed. Current policy risks eviscerating medical privacy and confidentiality and will undermine not only a soldier's quality of life, but also, mission readiness. The paper recommends changing the current guidance to better comport with strategic objectives.

COMMANDER'S "RIGHT TO KNOW" HEALTH INFORMATION: A STRATEGICALLY FLAWED INNOVATION

> Commanders play a critical role in the health and well-being of Soldiers, and therefore, require sufficient information to make informed decisions about fitness and duty limitations.[1]
>
> —Gen. Peter W. Chiarelli,
> Vice Chief of Staff, US Army

A battalion commander asks his unit physician's assistant (PA) for the names of all soldiers who have visited behavioral health[2] services and all soldiers who are on any behavioral health medications. Armed with the recently coined "commander's right to know" certain health information, the commander believes the requested information will allow him, and his subordinate leaders, to best take care of these soldiers. SPC Jones, who had earlier scheduled an appointment with a behavioral health provider, learns of the commander's new policy and cancels his appointment.

The United States military's greatest strategic asset is its Soldiers, Sailors, Airmen and Marines.[3] One of the Army's strategic objectives, "sustain[ing] an all-volunteer force composed of highly competent Soldiers that are provided an equally high quality of life,"[4] has become increasingly challenging to accomplish in light of nearly ten years of persistent conflict and impending budget cuts.[5] Key to a service member's (SM) quality of life and a military unit's performance is the relationship between SMs and their leaders. To be effective, commanders, senior non-commissioned officers and other unit leaders need to know and understand their troops. Thus quality leaders strive to learn as much about their personnel as possible. At the same time, privacy is widely recognized as a fundamental right of all Americans. As Justice Louis Brandeis observed, the "makers of the Constitution conferred the most comprehensive of rights

and the right most valued by all civilized men—the right to be let alone."[6] Individual service members, like all United States citizens, have the desire, and sometimes the legal right, to keep certain information private. In the context of medical care, privacy and confidentiality between patients and healthcare providers advance important societal objectives. Compelling practical, ethical and legal reasons justify such privacy, particularly in a military context where the negative stigma associated with seeking behavioral health services is acute. This paper addresses the strategic implications of the tension between a leader's interest in gathering his subordinates' personal medical or mental health information and the subordinate's interest in privacy.

This paper asserts that current Army and DOD guidance governing disclosure of service members' personal health information is strategically flawed. Current policy risks eviscerating medical privacy and confidentiality and will undermine not only a soldier's quality of life, but also, mission readiness.

The next section of this paper discusses how privacy, generally, and, in particular, informational privacy, advances important societal values and interests. Section three addresses the perspectives of three key stakeholder groups: healthcare providers (with emphasis on military providers), military leaders, and service members in their roles as patients or potential patients. Next, the paper provides the legal and regulatory provisions governing military health information disclosure. The paper then analyzes and evaluates the current military guidance. The paper finds that strategically the current approach undermines important policy ends, including, the military's objectives to maintain a high quality volunteer force and to reduce stigma associated

with seeking behavioral health services. The paper concludes with recommendations to alter the current guidance to better comport with strategic objectives.

The Value of Privacy

Philosophers, ethicists, and legal scholars have recognized the importance and value of "privacy" to individuals and to society. While no consensus exists regarding a definition of privacy, certain characteristics have coalesced around what Justice Louis Brandeis, famously, referred to as the "right to be let alone."[7] Privacy is a "state or sphere where others do not have access to a person, their information, or their identity."[8] "Informational privacy" revolves around the ability to control when, how and to what extent personal information is communicated to others.[9] Confidentiality, which protects certain communications between individuals, is a subset of privacy.

Some commentators, particularly ethicists, see privacy as a basic human right based on the principal of personal autonomy.[10] From that perspective, privacy is worthwhile, in and of itself, because it advances such "fundamental values" as "the ability to make decisions, individuality, respect, dignity and worth as human beings."[11]

More commonly, privacy is viewed as beneficial because it advances more pragmatic objectives. For individuals, protecting privacy may not only protect an abstract sense of dignity but also serves to avoid stigma or embarrassment, and may also prevent discrimination or economic harm.[12] In addition, privacy helps foster healthy relationships.[13] Finally, several commentators have observed that a community that respects privacy rights is the type of a free society in which Americans want to live.[14]

Privacy, in the context of healthcare, "has come to be linked most directly with one's ability to make decisions related to one's body without intrusion by others."[15] Medical data is often particularly intimate. For the reasons discussed above – stigma,

embarrassment, discrimination and economic harm – citizens are uniquely concerned about maintaining privacy of their health information.[16] Individuals who do not trust that medical information will be kept confidential are more likely to avoid going to doctors, withhold information from their healthcare providers, ask their healthcare providers to not record certain information or request physicians to mischaracterize diagnoses.[17] Therefore, protecting health data improves doctor-patient communication and improves the provision of healthcare itself, benefitting individuals and society. Thus, very practical consequences, impacting individuals and public health, result from the failure, or perception of failure, to protect personal health information.

Doctor's Perspective—Privacy and Confidentiality.

Deeply ingrained ethical standards have created a culture within the medical community that deeply respects medical privacy and confidentiality. The need for medical privacy has long been recognized. The Hippocratic Oath explicitly requires that a physician "not divulge" secrets that "ought not be spoken about."[18] More broadly, the deeply ingrained "nonmaleficence" concept, "do no harm," undergirds the ethical principal of privacy because privacy breaches could embarrass, stigmatize or result in discrimination of the patient or third parties.[19]

The American Medical Association (AMA) treats confidentiality as a subset of privacy. While "confidentiality" pertains to "information told in confidence or imparted in secret," privacy involves any "information that is concealed from others outside of the patient-physician relationship."[20] Thus, "privacy" would include a patient's "thoughts or feelings,"[21] a doctor's observations or laboratory results, while confidentiality pertains primarily to communications between doctor and patient.

The AMA Code of Medical Ethics protects medical privacy and confidentiality. It provides that physicians "shall safeguard patient confidences and privacy within the constraints of the law."[22] In addition to legal constraints, the standard recognizes that privacy must be balanced against the efficient provision of care.[23]

Privacy, from the medical ethics perspective, is considered a right of every individual.[24] Protecting privacy serves as a "fundamental expression of patient autonomy" and builds "the trust that is at the core of the patient-physician relationship."[25] In contrast, confidentiality arises from a formal or informal agreement between a physician and patient that information divulged by another person will not be further disseminated. The obligation of confidentiality arises with the relationship between patient and doctor.[26]

Confidentiality is a core precept in the practice of medicine.[27] The AMA Ethics Code provides that normally a physician should not disclose confidential information because confidentiality is necessary to "effectively provide needed services."[28] The Code recognizes, however, that "overriding considerations" allow physicians to disclose confidences without the consent of the patient.[29] One "overriding consideration" permitting disclosure is when a "patient threatens to inflict serious physical harm to another person or to him or herself and there is a reasonable probability that the patient may carry out the threat."[30] Thus, AMA ethical guidance recognizes the tension between safeguarding patient confidences and public policies requiring disclosure.[31] When the law requires disclosure, physicians must disclose only minimal confidential information.[32]

The AMA Ethics guidelines urge physicians to attempt to change any law that is inconsistent with the best interests of a patient.[33] Regarding confidentiality, physicians faced with legal requirements contrary to ethics principles should "advocate for the protection of confidential information and, if appropriate, seek a change in the law."[34]

According to the AMA Council on Ethical and Judicial Affairs, the practical benefits of confidentiality flow from reciprocal duties between doctor and patient. Confidentiality's "value in the context of the patient-physician relationship stems partly from the need for patients to trust their physicians, and for physicians to express their loyalty to patients."[35] According to the AMA, a physician's ethical obligations center on advancing the patient's interest. In contrast, the law generally seeks to advance the public's interests.[36] As seen in the next section, military healthcare providers must advance the interests of a third entity: the Armed Forces.

Challenges Unique to Military Health Care Providers

Military healthcare providers (HCP) face the problem of "dual loyalty," also known as "mixed agency" or "conflict of interests."[37] Two sets of professional ethics govern the conduct of military HCPs – one demands loyalty to the military mission, the other to the individual patient. Uniformed healthcare providers differ from their civilian counterparts because they are commissioned officers, dedicated to the military mission with military duties and part of the military hierarchy.[38] While in most situations the two sets of ethical demands point in the same direction, at times they conflict. Resolving such conflicts may involve law, ethics and personal moral discretion. Unfortunately, as one commentator observed, the military fosters "an organizational culture that is often disinterested in, if not overtly hostile, to the concept of service member confidentiality."[39]

In *Military Medical Ethics*, Edmund Howe, describes three categories of ethical dilemmas. The "first category is one in which military physicians should exercise no discretion because the needs of the military should be absolute."[40] When disaster would result from advancing an individual patient's interests over the military's needs, such as loss of hundreds of lives, defeat in battle or perhaps loss of war itself, then the physician must disregard the patient's interest. For example, military doctors may ethically treat soldiers with combat fatigue in such a way that encourages them to return to combat.[41] The "military needs should prevail because the consequences of not doing so are unthinkable. The national security interest, and therefore the 'military necessity,' is compelling."[42]

At the other extreme, lie circumstances in which a military physician's medical ethics must mirror a civilian colleague's. For example, a military physician should not disclose that a military patient told the physician, in the course of treatment, that he was having an extra-marital affair.[43] In that instance, the physician's duty of confidentiality defeats any perceived military advantage. Because the "patient has a clear medical interest" and the "military has virtually none,"[44] the physician must adhere to his civilian role medical ethical responsibilities.

Howe indicates that scenarios at either end of the spectrum are rare.[45] Rather, the military physician is more likely to face challenges requiring the exercise of discretion. In this "area, physicians must weigh choices and obligations to ensure the best treatment possible for patients within the context of military interests."[46] Confidentiality issues often fall into this category. Howe discusses balancing military needs with patient confidentiality in the context of treating pilots[47] or senior officers.[48]

Each has tremendous responsibility for the lives and safety of others. Nonetheless, if information learned from these patients has minimal impact on the military mission, a doctor would not necessarily have to disclose confidential information. Howe discusses several questions a doctor should consider in exercising discretion, including: are there specific laws or regulations governing disclosure; what is the likely gain to the military compared to the harm to the patient; what is the risk to the physician of disclosure or non-disclosure; what informed consent did the patient provide; what other "promise," implicit or explicit, existed between patient and physician.[49]

Health care providers, of course, are only a small sub-set of the military community. The next section addresses health information privacy from the perspectives of military leaders and service members.

Unique Military Environment: Leader's Perspective and Service Member's Reduced Expectation of Privacy

Courts have "long recognized that the military is, by necessity, a specialized society separate from civilian society."[50] As a result of the "different character of the military community and of the military mission," Constitutional protections apply differently to military members.[51] Though no court has ruled on the right of information privacy in the military, undoubtedly, the right would be applied differently than in the civilian world.

The highest military court has recognized "the responsibility and accountability of commanders for the successful conduct of military operations."[52] In the context of searches and seizures, military courts have recognized the far-reaching roles and responsibilities of commanders: "A military commander has responsibilities for investigation and for law enforcement .... Also, he has responsibilities for the welfare

and combat readiness of the personnel under his command."[53] Not only must commanders accomplish the most challenging combat missions, but they must also take care of the Soldiers, Sailors, Airmen and Marines under their command. Army commanders are responsible for the welfare of soldiers at various levels. By Army regulation, "Every leader will— . . . c. Ensure the physical, moral, personal, and professional wellbeing of subordinates."[54] Further, the depth of understanding which commanders and subordinate leaders are expected to reach is astonishing. For example, "Leaders must monitor assigned personnel routinely and become familiar enough with unit members to assess the personal risk factors of—Financial problems; Alcohol misuse; Immaturity; Relationship problems."[55]

Key to any military unit's performance is the relationship between service members (SMs) and their leaders. To take care of a SM at a personal level, leaders need to ask questions and get information from various sources. Medical data will often be relevant. As the Army's Vice Chief of Staff observed "Commanders play a critical role in the health and well-being of Soldiers, and therefore, require sufficient information to make informed decisions about fitness and duty limitations."[56] Greater knowledge gives the commander better tools to help the soldier.

Although the courts have not addressed information or medical privacy in a military environment, their analysis of privacy in the Fourth Amendment context (search and seizure law) is instructive. In the Fourth Amendment context, the "'expectation of privacy' ... is different in the military than it is in civilian life."[57] History, custom and the role of the commander, result in lawfully vesting commanders with substantial authority and concomitantly limiting service members' reasonable expectation of privacy.[58]

Application of "the Fourth Amendment" must "take into account the exigencies of military necessity and unique conditions that may exist within the military society."[59] As a result, a commander can not only order a search based on probable cause, but also has the authority, unprecedented in the civilian world, to order an inspection of a whole or part of a unit to determine "security, military fitness, or good order and discipline."[60] These authorities flow from the service member's reduced expectation of privacy and the far-reaching role of the military commander.[61]

Case law, however, recognizes that effective leadership is not primarily defined by discipline, punishment or legal constraints. Rather, a critical "aspect of successful leadership is concern for the welfare of subordinates. Loyalty in a military unit ... is a two-way street."[62] That is, the relationship between soldiers and leaders, like the relationship between doctor and patient, is based on trust. A "commander who approves or even tolerates arbitrary invasions of the privacy of his subordinates is not demonstrating the brand of leadership likely to command the loyalty or produce the high morale associated with a combat-ready organization."[63] Although the court was discussing privacy in the context of searches and seizures, the same concept applies to medical information privacy: effective leadership recognizes that honoring privacy reflects respect for service members' dignity, improves relationships and builds better units.

Service Member As Patient: Particular Sensitivity To Disclosure Of Health Information.

Although service members have a lesser expectation of privacy than civilians under the law, they may have greater subjective need for medical privacy and confidentiality. "Alarming levels" of behavioral health and substance abuse problems have been reported among service members returning from Operations Enduring

Freedom and Iraqi Freedom.[64] The "signature" injuries of these conflicts are not always visible. Psychological injuries, foremost among them Post-Traumatic Stress (PTS), and neurological injuries, primarily Traumatic Brain Injury (TBI), have proven challenging to identify and treat. One of the primary barriers to effective care of PTS and TBI has been the stigma, or perception of stigma, associated with service members seeking behavioral health services. Keeping behavioral health information confidential is one critical means to reduce the stigma of seeking behavioral health services.

Service members are concerned that seeking mental health treatment would damage their careers and influence how they are viewed by unit leadership.[65] In June 2007, the Department of Defense Mental Health Task Force (MHTF), reported, "[s]tigma [associated with seeking mental health services] in the military remains pervasive and often prevents service members from seeking needed care."[66] The Army's comprehensive study on Health Promotion/Risk Reduction/Suicide Prevention (HP/RR/SP Report) defined stigma as "the perception among leaders and Soldiers that help-seeking behavior will either be detrimental to their career (e.g., prejudicial to promotion or selection to leadership positions), or that it will reduce their social status among their peers."[67] Stigma contributes to soldiers' failure to obtain needed mental health services.[68] The Mental Health Task Force identified, "Dispelling Stigma," as its first recommendation to build a culture of support for psychological health[69] and thereby improve the efficacy of mental health services provided to Service Members.[70] Failure to obtain behavioral healthcare contributes to increased suicides, untreated PTS and TBI, and a host of other soldier and soldier-family problems.

Over the last two years, both DOD and the Army have made concerted efforts to reduce the stigma associated with a service member seeking behavioral health assistance. The Vice Chief of Staff of the Army (VCSA), General Peter Chiarelli, has made improved behavioral health, generally, and reduction of stigma, more particularly, among his top priorities.[71] The VCSA has spoken and written frequently on reducing the stigma of "seeking help."[72] He has stated, the Army must "reduce the stigma associated with help-seeking behavior."[73] Attention from military leaders advances a cultural change reducing the stigma of seeking mental health assistance.[74]

Recognizing the benefits that flow from allowing service members to keep mental health services confidential, DOD recently revised the mental health question on the standard security questionnaire.[75] As of March 2010, the revised question exempts from reporting any counseling "strictly related to adjustments from service in a military combat environment" and explicitly states, "Mental Health counseling in and of itself is not a reason to revoke or deny a security clearance."[76] DOD recognized that service members perceive that disclosure of mental health information will have a negative impact on obtaining (or retaining) a security clearance and hence a negative impact on their career. This is a concrete example of the economic harm (or at least the perception of such harm) that could result from disclosure, even self-disclosure, of medical information.[77]

Three programs, two from the Army and one from DOD, explicitly seek to reduce stigma by enhancing privacy or confidentiality. First, the Army initiated the Virtual Behavioral Health Program where soldiers can obtain behavioral health consultations through video-conferencing.[78] The counseling sessions can take place from a service

member's home during non-duty hours. By creating a method to obtain behavioral health services in private, outside of the service member's unit environment, this program seeks to reduce stigma. Second, the Confidential Alcohol Treatment Education Pilot (CATEP) provides confidential means for Soldiers to refer themselves for Alcohol Substance Abuse Program (ASAP) treatment without command notification and subsequent administrative or disciplinary action.[79] The program was designed to allow soldiers to seek help without fear of damage to their careers.[80] The CATEP Program was specifically designed "in response to the belief that command stigma originating from supervisors and peers represents a significant barrier to treatment."[81] A preliminary examination of CATEP revealed the program's confidentiality provisions have increased the likelihood soldiers will seek treatment.[82] Finally, Military OneSource[83] offers up to twelve sessions of face-to-face, telephonic or on-line counseling outside of the Tricare system and without notification to the chain of command. Confidentiality is maintained except to meet legal obligations mirroring those in a civilian context.[84] Military OneSource counselors will keep information private except to prevent harm to the patient or others, or to report family maltreatment, substance abuse or illegal activities.[85]

The principles and interests discussed in this and previous sections form the basis for laws and regulations governing health information privacy. The following section addresses United States' case law and regulations and the military's implementation thereof.

Legal and Regulatory Provisions

Case Law. According to the information privacy legal scholar, Daniel Solove, the tort of breach of confidentiality arose in the early 20th Century and by the end of the

century had been recognized by most American jurisdictions.[86] He described the parameters of the tort as "a cause of action against a physician for the unauthorized disclosure of confidential information unless the disclosure is compelled by law or is in the patient's interest or the public interest."[87] In 1977, in *Whalen v. Roe*, the Supreme Court recognized a constitutional privacy "interest in avoiding disclosure of personal matters."[88] Very recently, the Supreme Court, "assume[d], without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen*."[89] Although the Supreme Court has never expounded on the limits of such a right, some federal appellate courts have broadly interpreted the right to informational privacy.[90] In sum, the law values medical information privacy and protects against inappropriate disclosures of confidential information by both physicians and government actors.

HIPAA Privacy Rule. President Clinton signed the Health Insurance Portability and Accountability Act (HIPAA) on August 21, 1996.[91] The Department of Health and Human Services (HHS) published regulations, known collectively as the "Privacy Rule," governing privacy and confidentiality of medical information on August 14, 2002.[92]

The drafters intended the regulations to create a scheme that sufficiently protected individual health information while allowing the flow of information necessary to promote high quality care.[93] According to HHS, "a major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed."[94] The HIPAA rules apply to health plans and healthcare providers,[95] including military healthcare providers.[96] Referred to as "Protected Health Information (PHI)," HIPAA protects information that identifies an

individual and “relates to” the “individual’s past, present or future physical or mental health or condition [or] the provision of healthcare to the individual.”[97]

A covered entity may disclose PHI under two general circumstances: the individual patient authorizes disclosure in writing or “as the Privacy Rule permits.”[98] A covered entity may, but is not required to, disclose PHI without an individual’s authorization under various limited circumstances under HIPAA.[99] In most instances, “covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.”[100] Covered entities may disclose PHI to healthcare providers for treatment purposes.[101] Further, the privacy rule permits, but does not mandate, disclosure, without an individual’s permission for “12 national priority purposes.”[102] Each purpose has its own rules, “striking the balance between the individual privacy interest and the public interest need” for the information.[103] These purposes include: when required by law;[104] for public health purposes;[105] regarding victims of abuse;[106] for health oversight activities;[107] in judicial and administrative proceedings;[108] for law enforcement purposes under certain circumstances;[109] to prevent a serious and imminent threat to a person or the public;[110] for certain essential government functions.[111]

The Privacy Rule contains a more restrictive provision for psychotherapy notes. Without the permission of the patient, the Privacy Rule limits disclosure solely “to avert[ing] a serious and imminent threat to public health or safety, to a health oversight agency ... or as required by law.”[112]

Consistent with the ethical standards discussed above, a central aspect of the Privacy Rule is the principle of “minimum necessary” disclosure.[113] That is, a “covered

entity must make reasonable efforts to ... disclose, only the minimum amount of PHI needed to accomplish the intended purpose of the ... disclosure."[114]

DOD and Army Implementation of HIPAA. The HHS-developed Privacy Rule explicitly allows the military to disclose PHI of military personnel "for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission."[115] DOD implemented HIPAA in DOD Regulation 6025.18-R, DOD Health Information Privacy Regulation in January 2003.[116] The Regulation expounds on how the HHS' exception applies to the military.[117] The Regulation set forth five bases for which PHI may be disclosed absent service member authorization. Two were quite specific: "To carry out [Joint Medical Surveillance] activities" and to "report on casualties in any military operation." Three others, however, broadly describe permitted disclosure circumstances:

> To determine the member's fitness for duty ... To determine the member's fitness to perform any particular mission, assignment, order, or duty, including compliance with any actions required as a precondition to performance of such mission, assignment, order, or duty.... To carry out any other activity necessary to the proper execution of the mission of the Armed Forces.[118]

On July 2, 2009, DOD, acting on recommendations of the DOD Mental Health Task Force (MHTF) published a directive-type memorandum (DTM) entitled "Revising Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Military Personnel."[119] The MHTF found that the "low thresholds for notifying commanders of Service members'" mental healthcare resulted in "members not seeking treatment, yet continuing in their operational roles, while their problems" [120] grew worse. The directive sought to better balance patient confidentiality with a commander's need to know information for operational and risk management purposes.[121] The directive,

either intentionally or inadvertently, introduced the term “commander’s **right to know**” (emphasis added) in regards to certain health information. This term does not appear, previously or subsequently, in any other context.[122]

The DTM delineated eight mental health conditions requiring a healthcare provider to proactively notify a commander of the member’s condition: serious risk of self-harm; serious risk of harm to others, including child abuse or domestic violence; serious risk of harm to a specific military operational mission; members in the Personal Reliability Program or a position of similar sensitivity or urgency; inpatient care; member is experiencing an acute medical condition that interferes with duty; member has entered a substance abuse treatment program; and, a command-directed mental health evaluation.[123] Finally, consistent with the Privacy Act, the directive requires commanders to restrict further dissemination of the disclosed information to personnel with a need for the information.

In early 2010, the Army issued a Rapid Action Revision (RAR) of Army Regulation 40-66 (AR 40-66 Revision), *Medical Record Administration and Healthcare Documentation*. The revision emphasized new requirements placed on healthcare providers to communicate with commanders. The Regulation directs unit surgeons, “when available and appropriate” to be involved in the “communication of a Soldier’s PHI to a unit commander.”[124] More pointedly, the regulation directed unit surgeons to “provide timely and accurate information to support unit commanders’ decision making pertaining to the health risks, medical fitness, and readiness of their Soldiers.”[125]

The AR 40-66 Revision set forth, in great detail, those regulatory programs authorizing disclosure within DOD of PHI without the consent of soldiers. Under the

category “when required by law or Government regulation,” the regulation revision listed 18 specific regulatory bases permitting disclosure.[126] Further, it included a “catch-all” authorization, i.e., “[a]ccording to other regulations carrying out any other activity necessary to the proper execution of the Army’s mission.”[127] Finally, AR 40-66 provides eight, non-exclusive, situations in which MTF Commanders “will proactively inform a commander of a soldier’s minimum necessary PHI:”

> To avert a serious and imminent threat to health or safety of a person, such as suicide, homicide, or other violent action[128]... (b) A high risk Soldier receives multiple behavioral health services and requires high risk multi-disciplinary treatment plans.[129] ... (c) Medications could impair the Soldier’s duty performance.[130] ... (d) The Soldier’s condition impairs his/her performance of duty.[131] (e) The injury indicates a safety problem or a battlefield trend. (f) There is a risk of heat/cold injury. (g) The Soldier requires hospitalization. (h) The Soldier is categorized as seriously ill or very seriously ill.[132]

On 28 May 2010, the VCSA published a message on PHI.[133] The message was intended to “improve information and data disclosure.”[134] The message is commander-focused, emphasizing that “commanders play a critical role in the health and well-being of their soldiers.”[135] As a result, commanders “require sufficient information to make informed decisions about fitness and duty limitations.”[136] The message includes one of the broadest descriptions of when health care providers must disclose PHI by requiring medical personnel to provide “timely information ... when health problems exist that **may impair a soldier’s fitness for duty**” (emphasis added).[137]

The message recognizes limits on releasability and directs that the soldier’s “right to the privacy of his/her” PHI, be balanced with mission requirements and the “commander’s right to know.”[138] The message recognizes that “it would be counterproductive for soldiers to perceive increased stigma, or not seek medical care, because of inappropriate release of PHI.”[139] The message states that “collaborative

communication" between commanders and "healthcare providers is critical to the health and well-being of our soldiers."[140] The message directs healthcare providers to "not limit communication to 'sick call slips,' but should speak with commanders when required."[141]

Based on the VCSA's message, the Army Medical Command and Office of the Surgeon General published Policy Memorandum 10-042, "Release of Protected Health Information to Unit Command Officials."[142] The policy directs medical commanders to "provide timely and accurate information to support unit commanders' decision-making pertaining to the health risks, medical fitness and readiness" of soldiers.[143] The policy further encourages communication between command and medical personnel. The message captures regulatory guidance, previously discussed in this paper, authorizing disclosure, including five circumstances in which the minimum necessary disclosure of PHI may be made absent soldier authorization and **22** examples of "regulatory and command management programs that do not require a Soldier's authorization for PHI disclosure."[144]

Finally, service members' health information is protected by both the Privacy Act and DOD's regulation implementing HIPAA.[145] If PHI is disclosed within DOD pursuant to HIPAA, that information is then protected from further dissemination only by the Privacy Act.[146] Thus, if doctors disclose PHI to commanders, HIPAA rules no longer apply, but instead the relatively more lenient standards of the Privacy Act protect such information from additional disclosure.[147] Within DOD, disclosure would be permitted to anyone with an official need to know.[148]

Analysis and Evaluation

Analysis of the current DOD and Army health privacy guidelines leads to two major conclusions. First, recent changes in regulation and policy risk substantially

reducing healthcare privacy and confidentiality in the military. Second, less privacy will undermine military readiness. This second conclusion stems from several related causes: less privacy directly contradicts efforts to reduce the stigma of seeking behavioral health services and hence will undercut efforts to address Post Traumatic Stress, Traumatic Brain Injury and related wartime maladies; less privacy will undermine trust and loyalty between service member and leader; less privacy will undermine the doctor–military patient relationship, putting military healthcare providers in an untenable ethical position and reducing the effectiveness of medical care; and, reduced privacy will negatively impact on retention of service members.

Interestingly, recent guidance purports to recognize the need to balance a service member's interest in privacy with a leader's interest in gaining information. The recent DTM, for example, states that its purpose is to address the "low thresholds" that exist allowing healthcare providers to disclose PHI to leaders. Similarly, the VCSA's message expresses concern that "we must balance the soldier's right to the privacy of his/her protected health information (PHI) with mission requirements and the commander's right to know. It would be counterproductive for soldiers to perceive increased stigma, or not seek medical care, because of the inappropriate release of PHI."[149] Unfortunately, the recent guidance, taken together, strikes the wrong balance and will cause the perception, at a minimum, of a "pass-through" of information between doctors and commanders. Some of the very evils of which the VCSA warns – increased stigma and failure to seek medical care – and others, will come to fruition.

The DOD and the Army have taken several steps, each discussed individually below, to substantially expand service members' PHI subject to disclosure. First,

military guidance broadly defines mission needs by mandating or permitting disclosures pursuant to a wide variety of regulations. Second, whereas most of the civilian Privacy Rule disclosures are permissive, DOD introduces numerous mandatory disclosures which military HCPs must proactively disclose. In addition, DOD recently asserted that commander's have a "right to know" PHI under certain circumstances. Finally, the Army recently promulgated guidance requiring communications between commanders and healthcare providers concerning a service member's medical status.

Recent Changes Risk Substantially Reducing Health Care Privacy in the Military. The initial approach of the 2003 DOD regulation concerning privacy left the door open for a substantially more disclosure-friendly approach than corresponding civilian rules. Disclosure of PHI is permitted on several vague and amorphous grounds: "fitness for duty," "fitness for a particular mission," and "to carry out any other activity necessary to the proper execution of the mission." Nonetheless, this difference alone did not substantially impact military medical privacy in a negative manner. The culture of confidentiality and privacy, instilled in all physicians, successfully counter-balanced the more disclosure-permitting DOD regulation. Three recent publications in the area of military healthcare privacy, however, when viewed together risk vastly and inappropriately, expanding the information that providers disclose to commanders and other unit leaders.

First, AR 40-66 and the recently published OTSG Message provide a lengthy list of circumstances permitting disclosure of PHI. This list risks the disclosure exceptions swallowing the privacy rule. Even though each of these exceptions only allows information to be disclosed for a particular regulatory purpose, once released from

healthcare providers, the information is no longer protected by HIPAA. Instead, only the Privacy Act stands in the way of subsequent disclosures. Further, while the medical profession instills in its members a culture that values confidentiality, that cultural value is not widely shared throughout the military. Therefore, once released out of medical channels, information is more likely to be widely shared.

Secondly, the 2009 DOD DTM gave commander's a "right to know" certain health information. The Army quickly adopted the term and the VCSA used it in his 2010 VCSA memorandum. In addition, the VCSA memorandum adopted one of the broadest approaches to disclosure, directing military HCPs to provide "timely information ... when health problems exist that may impair a soldier's fitness for duty."[150] Finally, the VCSA urged additional communication between healthcare providers and commanders.[151]

The communication directive, coupled with the newly introduced commander's "right to know" and the extant lengthy list of permitted regulatory disclosures, risks medical professionals becoming, or at least being perceived as becoming, a "pass-through" to unit leaders for private medical information. The Army's emphasis on "communication" between healthcare providers and commanders will open the flood gates of information. "Minimum necessary" disclosure will wither in the face of person-to-person questioning from a commander.

Howe, writing on medical ethics, recognized that risk to HCPs is a factor to consider when determining whether confidentiality should be breached. Current regulation and policy suggest that military doctors will never risk harm, through military channels, for disclosing information. On the other hand, doctors will always be in fear that failure to disclose particular PHI will result in a negative consequence (i.e. violence

or suicide) and the HCP will be blamed. At the same time, substantial pressure can be put on doctors as commander's exercise their newly created "right to know" through the recently mandated "collaborative communications." Soldiers, meanwhile, have little practical recourse if information is inappropriately disclosed. The only formal complaint apparatus is through the Department of Health and Human Services. In theory, doctors could face discipline from their non-military licensing authorities. However, if military medical channels support military HCPs, state licensing organizations are unlikely to second-guess the military evaluation.

Military HCPs will feel constrained to disclose rather than "advocate for the protection of confidential information." Military HCPs are unlikely to seek to change aspects of the confidentiality rules, even if they are inconsistent with the best interests of a patient.

Less Privacy Undermines Military Readiness.

> The Army's strategic objectives clearly state the Army's purpose: ... sustain an all-volunteer force composed of highly competent Soldiers that are provided an equally high quality of life; ... The means of this strategy are people more specifically, leaders... These leaders represent the means for the Army to achieve its desired end.[152]

Readiness is perhaps the most challenging area in which to balance privacy and disclosure. On the one hand, privacy helps build strong and healthy relationships. On the other hand, disclosure may be necessary for the very safety of unit members. The views of both the individual soldier-patient and his fellow unit members must be considered.

Many facets of a service member's life are exposed to peers and unit leaders. Further, many decisions that a civilian could make freely are controlled in the life of a

service member. Few areas are kept "private." Service members, however, have the same human needs to maintain dignity and personal autonomy and avoid embarrassment. In the small and often tight-knit nature of a military community, service members may be particularly sensitized to avoiding the embarrassment associated with some medical or mental health conditions. Further, service members clearly perceive that discrimination and economic harm may result if certain conditions become well-known. Maintaining privacy of medical information contributes to a positive self-image of soldiers. A military society that maintains medical privacy appropriately is one that service members will want to inhabit. Therefore, secondary effects of greater confidentiality protections would be a better quality of life for service member-patients and higher retention of these service members in the military.

Commanders and other unit leaders, on the other hand, are charged with also protecting the interests of the peers and comrades of these service member patients. These fellow Soldiers, Sailors, Marines and Airmen will take solace knowing that the commander knows which personnel are on medications that may impact the mission. They would be reassured to know that the unit physician informed the commander that one of their peers needs to be taken off of a mission because he may break down due to a physical or behavioral condition. Therefore, the military medical confidentiality scheme should never fully mirror the civilian one.

Broader disclosure undermines efforts to reduce stigma. DOD policy strives to "[e]liminate barriers to and the negative stigma associated with seeking counseling support."[153] The most specific and immediate defect associated with the broad disclosure approach is that it undercuts the effectiveness of the military's robust efforts

to reduce the stigma of seeking behavioral health services and to address PTS and TBI. The physical and mental health of military personnel is a critical component of maintaining both a high quality of life and top-notch competence. Unfortunately, as a result of the stigma associated with seeking behavioral health services, many service members avoid needed treatment. Embarrassment and fear of negative career repercussions contribute to stigma.

The military has gone a long way to protect privacy. Some recent efforts have taken the command structure out of the medical process. Both CATEP and Military One-Source, for example, allow soldiers to obtain treatment outside of traditional channels. Broader disclosure of health information to unit leaders runs directly counter to these and other recent stigma-reducing initiatives.

Broader disclosure undermines trust between a service member and his leaders. Like the commander who arbitrarily invades the physical space of a service member, lack of medical confidentiality risks eroding the professional trust relationship between a service member and his/her leadership. Although, commanders need to stay informed of serious medical or behavioral issues to accomplish their missions safely and to keep faith with the rest of the unit personnel, as discussed earlier, honoring medical privacy demonstrates that leaders respect service members' dignity and will improve relationships and build better units.

Broader disclosure also undermines trust between the military patient and his/her healthcare provider and puts doctors in an untenable ethical position. The broad disclosure rules and close communications between HCPs and commanders interfere with the duty of "physicians to express their loyalty to patients." The civilian HIPAA

Privacy Rule has a separate section for psychotherapy notes which severely restricts disclosure of such information. The military privacy rules make no distinction between psychotherapy data and other HCP information. In light of the stress service members endure, they would greatly benefit from "the trust that is at the core of the patient-physician relationship." Reduced medical privacy and confidentiality make this trust relationship difficult to establish and maintain. As a result, some service members will be reluctant to seek care or may withhold information, thus compromising the quality of care.

In too many instances, the Army guidance transforms permissive disclosures into mandatory ones, often requiring proactive disclosure. Very few of the civilian world exceptions to privacy embodied in the HIPAA Privacy Rule require disclosure – instead they merely permit disclosure. This allows medical professionals to exercise discretion in most circumstances. Military practitioners have substantially lost this discretion. By eliminating medical discretion, military doctors are emasculated, ethically. The black and white approach removes decisions from being based on medical judgment to being rule-driven or commander driven. Discretion is one of the hallmarks of a professional. Howe discusses how military "physicians must weigh choices and obligations to ensure the best treatment possible for patients within the context of military interests."[154] Ceding medical discretion to regulations or to non-medical commanders risks forcing healthcare providers to violate deeply held medical ethical norms dating back to the Hippocratic Oath. Finally, the disclosure-friendly approach undermines the healthcare professional's ethical responsibility to provide minimum information and to "advocate for

the protection of confidential information and, if appropriate, seek a change in the law."[155]

The discussion above does not suggest that military medical privacy and confidentiality should replicate the civilian context. In circumstances when the military environment is truly "specialized," for example during combat or training missions where lives are at risk, medical personnel must err on the side of disclosure. Importantly, as discussed below, **military** professionals will exercise discretion in determining when disclosure should occur.

Recommendations and Conclusion

This paper recommends five actions the Army should take to embed a culture that respects confidentiality as an important value. First, by regulation, the most important standards in HIPAA should be extended to commanders and other unit leaders. Currently, once commanders learn information from HCPs, only the Privacy Act restrains the subsequent disclosure of medical information. The more permissive Privacy Act disclosure threshold – "need to know" – provides less protection of sensitive medical or mental health information. Applying HIPAA would distinguish medical information from other personal data pertaining to service members. This distinction would have both a direct and indirect impact. Directly, the HIPAA Privacy Rule, as implemented in DOD and Army regulation and guidance, would place additional restraints on disclosure. Indirectly, requiring leaders to adhere to the same privacy code as medical professionals will give leaders exposure to the culture of confidentiality and privacy embedded in the health care profession. This change would, in particular, limit further dissemination of PHI under the many regulatory provisions authorizing disclosure for limited purposes.

Second, DOD and the Army need to more narrowly define several of the terms that allow disclosure. For example, “fitness for duty”, “fitness for a particular mission,” and “to carry out any other activity necessary to the proper execution of the mission” could be more precisely defined. Refinements should occur in two areas. Guidance should distinguish situations when lives are at risk, in combat or in garrison. In those instances, the disclosure threshold should be lower than circumstances when the risks are not as great. This distinction captures one important facet of the unique military environment. In addition, any new standard should explicitly balance the risk of harm with the likelihood of that harm occurring. Military health care providers should make that determination. Uniformed doctors will always be cognizant of the unique military context.

Third, medical policy-makers should limit the communications between HCPs and unit leaders regarding individual soldier PHI. Regulations should require notification to service member patients when doctors communicate with their commanders about the service member’s medical or behavioral health, unless the treating doctor determines that such notification would be harmful to the patient. In most instances, such notification to the service member should precede any communication between HCP and leader. Notifying patients, even if they do not have the ability to stop the disclosure, would restore a measure of autonomy and self-respect to the soldier-patient and reduce the negative impact of such disclosure on the doctor-patient relationship.

Fourth, all references to a commander's "right to know" should be revised to read "need to know." Such a change would better balance the interests of individual service member patients with the interests of unit leaders.

Fifth, discretion for disclosure decisions should be returned to health care professionals. Most disclosures beyond those authorized in the civilian context should be made discretionary. The factors discussed by Howe would be appropriate. The needs of the military as a "separate society" would remain in the forefront because **military** doctors, perhaps in collaboration with military attorneys, would be making the disclosure calculus. Further, except in cases of exigency, the "disclosure authority" should reside at least one supervisory level higher, in technical medical channels, than the treating HCP. This would reduce pressure on junior HCPs facing more senior commanders and unit leaders and would further inject a more mature "military" perspective in the decision making process.

The limits of medical privacy and confidentiality are challenging areas in a military society. Reasonable minds could certainly disagree on how to balance the powerful interests and equities in both directions. This paper concludes that DOD, and the Army in particular, has moved too far towards abandoning meaningful restraint on disclosure of protected health information. Without betraying the unique aspects of the military environment, recent changes to the rules and policies should be re-visited to better protect the personal health information of our Soldiers, Sailors, Airmen and Marines. In the long run, such changes will best advance the strategic objective of "sustain[ing] an all-volunteer force composed of highly competent [Service members] that are provided an equally high quality of life."[156]

Endnotes

[1] Vice Chief of Staff of the Army Pete Chiarelli, "VCSA Sends On Protected Health Information (PHI)," Memorandum for All Army Activities (ALARACT), Washington, DC, May 28, 2010.

[2] Traditionally, counseling and other treatments from psychologists, psychiatrists, social workers and other related professionals have been known as Mental Health services. In June, 2009, the Army directed all commands to use the term behavioral health, rather than mental health, for all official purposes. The change in terms "supports an Army-wide campaign to foster an environment of reduced stigma for soldiers who seek mental health care." Staff report, "Army required to say 'behavioral health'", June 27, 2009, http://www.armytimes.com/news/2009/06/army_mentalhealth_062609w/ (last accessed March 6, 2011). This paper uses the two terms, mental health and behavioral health, interchangeably.

[3] U.S. Department of Defense, *National Defense Strategy* (Washington, DC: U.S. Department of Defense, June 2008), 19. ("The Department's greatest asset is the people who dedicate themselves to the mission."). See also, U.S. Department of Defense, *Quadrennial Defense Review Report*, (*QDR*) (Washington, DC: U.S. Department of Defense, February 1, 2010), 16., providing, "America's men and women in uniform constitute the Department's most important resource" and "In order to succeed in today's wars and prepare for the future, the Department of Defense must ensure the long-term viability of the All-Volunteer Force, its most precious military resource." exec. sum. xi and 15, respectively.

[4] U.S. Department of the Army, *Army Leadership*, Army Regulation 600-100 (Washington, DC: U.S. Department of the Army, March 8, 2007), 1. See also, U.S. Department of the Army *2010 Army Posture Statement*, (Washington, DC: U.S. Department of the Army, February 2010), 7 ("Sustaining our all-volunteer force is our first imperative.... The Army is committed to ensuring that the quality of life of those who serve the Nation is commensurate with the quality of their service.").

[5] For example, the 2010 QDR posits as one of four "priority objectives" to, "preserve and enhance the All-Volunteer Force." Defense, *QDR*, exec. sum., v.

[6] Olmstead v. United States, 217 U.S. 438, 478 (1928).

[7] Olmstead v. United States, 217 U.S. 438, 478 (1928).

[8] Joy L. Pritts, "The Importance and Value of Protecting the Privacy of Health Information: The Roles of the HIPAA Privacy Rule and the Common Rule in Health Research," 3, http://www.iom.edu/~/media/Files/Activity%20Files/Research/HIPAAandResearch/PrittsPrivacyFinalDraftweb.pdf. The article breaks down privacy into four components: solitude, seclusion, anonymity and secrecy or reserve. Ibid., 2-3.

[9] Ibid., 4.

[10] For example, claims to privacy "are justified by rights of autonomous choice that are correlative to the obligations expressed in the principle of respect for autonomy." Tom L. Beauchamp and James F. Childress, *Principles of Biomedical Ethics,* 4th ed., (United States: Oxford University Press, 1994), 410, as found in Nicolas P. Terry, "What's Wrong With Health Privacy," Journal of Health and Biomedical Law 5, (2009): 4.

[11] Sharyl J. Nass, Laura A. Levit, and Lawrence O. Gostin, eds., *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research* (Washington: DC: National Academies Press, 2009), 77.

[12] Pritts, Protecting the Privacy of Health Information, 4. Economic harm usually entails concerns about insurance and employment. Ibid., 7.

[13] American Medical Association, Council on Ethical and Judicial Affairs (CEJA) Report 2-I-01, "Privacy in the Context of Health Care," (2001), 1 (privacy is a "necessary condition for maintaining intimate relationships that entail respect and trust, such as love or friendship.")

[14] Nass, et. al., *Beyond the HIPAA Privacy Rule*, 78.

[15] AMA CEJA Report 2-I-01, Health Care Privacy, 2.

[16] Pritts, Protecting the Privacy of Health Information, 5. Citing a recent survey, Pritts stated:

> 67% of respondents said they were concerned about the privacy of their medical records ... When presented the possibility that there would be a nationwide system of electronic medical records, 70% of respondents were concerned that sensitive personal medical-record information might be leaked because of weak data security, 69% expressed concern that there could be more sharing of medical information without the patient's knowledge and 69% were concerned that strong enough data security will not be installed in the new computer system.

Ibid. (internal citations omitted).

[17] Pritts, Protecting the Privacy of Health Information, 6, discussing results from the Forrester Research for the California HealthCare Foundation, National Consumer Health Privacy Survey (CHCF 2005 Survey) 2005.

[18] AMA CEJA, *Health Care Privacy*, 2, quoting a common version of the Hippocratic Oath: "What I may see or hear in the course of treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will kept to myself, holding such things shameful to be spoken about."

[19] Nass, et. al., *Beyond the HIPAA Privacy Rule*, 77.

[20] American Medical Association (AMA), "Code of Medical Ethics: Opinion 5.059 - Privacy in the Context of Health Care," June, 2002, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion5059.shtml (accessed March 6, 2011).

[21] AMA CEJA Report, *Health Care Privacy*, 2.

[22] AMA CEJA Report, *Health Care Privacy*, 3, citing, American Medical Association, "Principles of Medical Ethics," Principle IV, June 2001. Privacy in the context of healthcare encompasses at least four "forms": "(1) physical, which focuses on individuals and their personal spaces, (2) informational, which involves specific personal data, (3) decisional, which

focuses on personal choices, and (4) associational, which refers to family or other intimate relations. AMA CEJA, *Health Care Privacy*, 3-4.

[23] AMA Ethics Opinion 5.059, Health Care Privacy. The standard also provides that patients should be made aware of any "significant infringement on their privacy." Ibid.

[24] AMA CEJA Report 2-I-01, Health Care Privacy, 2.

[25] Ibid., 3-4.

[26] Ibid., 2.

[27] "Confidentiality remains widely acknowledged as a fundamental ethical tenet of medicine, as patients must be willing to confide sensitive and personal information to healthcare professionals." Ibid., 2.

[28] American Medical Association (AMA), "Code of Medical Ethics: Opinion 5.05 - Confidentiality," June, 2007, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion505.shtml (accessed March 8, 2011.)

[29] Ibid.

[30] Ibid.

[31] American Medical Association, Council on Ethical and Judicial Affairs (CEJA) Report, 4-I-06, "Opinion E-5.05, 'Confidentiality,' Amendment," November 2006, 2-3.

[32] AMA Ethics Opinion 5.05. In addition, physicians should inform patients about any disclosure of confidential medical information. Ibid.

[33] Ibid. In addition, AMA Ethics Principle III provides, "A physician shall respect the law and also recognize a responsibility to seek changes in those requirements which are contrary to the best interests of the patient." American Medical Association (AMA), Code of Medical Ethics Principle III, June 2001, at http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/principles-medical-ethics.shtml (accessed February 9, 2011).

[34] AMA Ethics Opinion 5.05. Psychologists receive similar ethical guidance under the American Psychological Association's Ethical Standards. American Psychological Association, Ethical Principles of Psychologists and Code of Conduct (2010 Amendments), Standard 4: Privacy and Confidentiality, http://www.apa.org/ethics/code/index.aspx (accessed March 6, 2011):

> 4.01 Maintaining Confidentiality. Psychologists have a primary obligation and take reasonable precautions to protect confidential information obtained through or stored in any medium, recognizing that the extent and limits of confidentiality may be regulated by law or established by institutional rules or professional or scientific relationship.
>
> 4.05 Disclosures. (a) Psychologists may disclose confidential information with the appropriate consent of the organizational client, the individual client/patient, or

another legally authorized person on behalf of the client/patient unless prohibited by law. (b) Psychologists disclose confidential information without the consent of the individual only as mandated by law, or where permitted by law for a valid purpose such as to (1) provide needed professional services; (2) obtain appropriate professional consultations; (3) protect the client/patient, psychologist, or others from harm; or (4) obtain payment for services from a client/patient, in which instance disclosure is limited to the minimum that is necessary to achieve the purpose.

[35] AMA CEJA Report 2-I-01, Health Care Privacy, 2.

[36] AMA CEJA Report 4-I-06, Confidentiality, 3.

[37] Military psychologists, in particular, face frequent and stark "dual identity" issues. The literature discusses "notable conflicts" between Department of Defense and American Psychological Association standards in the areas of "confidentiality, multiple relationships, informed consent, and serving the individual client's best interests." Brad W. Johnson, "Top Ethical Challenges for Military Clinical Psychologists," *Military Psychology* 20 (2008): 51. Confidentiality consistently emerges as an area of concern for uniformed clinical psychologists. Confidentiality is listed as one of the top two ethical issues confronting uniformed clinical psychologists. Mathew McCauley, Jamie Hacker Hughes, and Helen Liebling-Kalifani, "Ethical Considerations for Military Clinical Psychologists," *Military Psychology* 20 (2008): 11.

[38] McCauley, et. al., "Ethical Considerations for Military Clinical Psychologists," 10-11.

[39] Johnson, Top Ethical Challenges, 58. A 1992 study recounts a licensing board disciplining a military psychologist for a breach of confidentiality based on release of patient records long after the psychologist had departed the duty station at which he had rendered treatment. The study also discusses military discipline of a psychologist for failing to disclose information about an improper relationship involving a patient. Ibid., 51.

[40] Edmund G. Howe, "Mixed Agency in Military Medicine: Ethical Roles in Conflict," in *Military Medical Ethics*, ed. Thomas Beam and Linette Sparacino (Washington, DC: Office of the Surgeon General, United States Army at TMM Publications, 2003), 335.

[41] Ibid., 336. Howe provided other examples. Health care providers could require soldiers to take unproven pharmaceuticals (i.e. anthrax vaccine), Ibid., 337-8; Providers may ethically not tell the truth to soldiers in certain combat scenarios, Ibid., 338-9. For instance, at the onset of the first Persian Gulf War, military members were told that they needed an initial botulism vaccine with one or more follow-up vaccines. During the war, the military ran out of vaccines. Rather than tell the service members this truth, doctors told them that the initial vaccine would be sufficient. Finally, three situations all related to "Treating and Conserving the Fighting Strength" are ethically permitted: "(1) treating soldiers to return to duty; (2) setting treatment priorities in triage situations; and (3) removing unstable soldiers from combat." Ibid., 339-42.

[42] Ibid., 343.

[43] Ibid., 347. Another classic example in the literature, mooted by recent legislative changes, holds that a HCP should not provide a medical chart to a commander seeking to prove that a soldier is a homosexual. Ibid., 335.

[44] Ibid., 347.

[45] Regarding times when the "military" interest would automatically trump the patient's, Howe is quite explicit:

> these situations are quite uncommon and, at their core, involve the survival of society and its members.... This point bears repeating: Military physicians in the course of their military service are not likely to have to make many choices that place the needs of the military ahead of those of the patient. However, if and when that situation arises, military physicians ideally will have thought about it and will understand why they must do it, whether or not they personally agree.

Ibid., 335.

[46] Ibid., 344.

[47] Ibid., 344-5.

[48] Ibid., 345.

[49] Ibid., 344-5.

[50] Parker v. Levy, 417 U.S. 733, 743 (1974).

[51] Parker v. Levy, 417 U.S. 733, 758 (1974). The First, Fourth, Fifth, Sixth, and Seventh Amendment rights have all been found to apply differently to military members. Justin Holbrook, "Communications Privacy in the Military," *Berkeley Technology Journal* 25: (2010): 838 (mentioning each of these Amendments and providing a discussion for each). Judicial deference to Congress is nowhere greater than when Congress exercises its power to "make rules and regulations" for the Armed Forces. Weiss v. United States, 510 U.S. 163, 177 (1994) (judicial deference ... is at its apogee when reviewing congressional decision making in this area."). None of which is to say that the Bill of Rights, or other constitutional rights, do not apply to military members, they do. United States v. Middleton 10 M.J. 123, 126 -127 (Court of Military Appeals, 1981) ("It has often been said that the Bill of Rights applies with full force to men and women in the military service unless any given protection is, expressly or by necessary implication, inapplicable.").

[52] The court also recognized the commander's responsibility for the "maintenance of a high state of discipline ... necessary to persevere and prevail amidst the danger, death, destruction, and chaos of armed conflict." United States v. Benedict 55 M.J. 451, 456 (U.S. Armed Forces, 2001) (recognizing these responsibilities in the context of deviating from the Sixth Amendment right to a jury trial and allowing the commander to select court-martial panel members).

[53] United States v. Stuckey, 10 M.J. 347, 359 (Court of Military Appeals, 1981).

[54] U. S. Department of the Army, *Army Leadership*, Army Regulation 600-100 (Washington, DC: U. S. Department of the Army, March 8, 2007), 6.

[55] U. S. Department of the Army, *Combat and Operational Stress Control Manual for Leaders and Soldiers*, Field Manual 6-22.5 (Washington, DC: U.S. Department of the Army,

March 18, 2009), 2-18. This level of care extends as well to family members. United States v. Day, 66 M.J. 172, 175 (U.S. Armed Forces, 2008) (Commander has an "interest in and responsibility for the health and welfare of dependents residing in base housing over which he exercised command responsibility.").

[56] Vice Chief of Staff of the Army Pete Chiarelli, "VCSA Sends On Protected Health Information (PHI)," Memorandum for All Army Activities (ALARACT), Washington, DC, May 28, 2010.

[57] United States v. McCarthy, 38 M.J. 398, 401 (Court of Military Appeals,1993) citing Committee for GI Rights v. Callaway, 518 F.2d 466, 477 (D.C. Circ. 1975).

[58] United States v. Middleton, 10 M.J. 123, 127 (Court of Military Appeals, 1981), stating:

> In considering what expectations of privacy a service member may reasonably entertain concerning military inspections, we must recognize that such inspections are time-honored and go back to the earliest days of the organized militia. They have been experienced by generations of Americans serving in the armed forces. Thus, the image is familiar of a soldier standing rigidly at attention at the foot of his bunk while his commander sternly inspects him, his uniform, his locker, and all his personal and professional belongings.

[59] United States v. Middleton, 10 M.J. 123, 127 (Court of Military Appeals, 1981).

[60] Mil. R. Evid. 313.

[61] United States v. Stuckey 10 M.J. 347, 360 (CMA, 1981), providing:

> "Military custom," so defined, has long granted military commanders broad powers of search and seizure.... The existence of that custom clearly imposes some limitation on a serviceperson's reasonable expectation of privacy. ... the commander's long-recognized power to authorize searches within the area of his command is generally viewed as derived from and correlative with his position and responsibilities in the military community which, of course, is "a specialized society separate from civilian society." (citations omitted).

[62] United States v. Stuckey 10 M.J. 347, 359 -360 (CMA, 1981).

[63] United States v. Stuckey 10 M.J. 347, 359 -360 (CMA, 1981).

[64] Deborah Gibbs and Kristine Rae Olmstead, "Preliminary Examination of the Confidential Alcohol Treatment and Education Program," *Military Psychology* 23, no. 1 (January-February 2011): 97. The Quadrennial Defense Review recognized these concerns as well:

> Years of war have significantly stressed our military personnel and their families. Although a strong sense of purpose and demonstrated operational excellence are shared across all Services and ranks, indicators of strain on the force—from retention levels in key commissioned and noncommissioned officer ranks, to increased rates of combat stress and substance abuse, and to even more tragic outcomes such as increased levels of suicide and divorce—are cause for concern.

U.S. Department of Defense, *Quadrennial Defense Review Report*, (Washington, DC: U.S. Department of Defense, February 1, 2010), 16.

[65] Gibbs and Olmstead, "Confidential Alcohol Treatment and Education Program," 98.

[66] U.S. Department of Defense Task Force on Mental Health, *An Achievable Vision: Report of the Department of Defense Task Force on Mental Health*, (Falls Church, VA: Defense Health Board, June 2007), exec. sum. 3.

[67] Army Health Promotion, Risk Reduction, and Suicide Prevention Report 2010 (Washington, DC: Department of the Army, July 30, 2010) (hereinafter Army HP/RR/SP Report), 22.

[68] Task Force on Mental Health, *An Achievable Vision*, 15.

[69] Task Force on Mental Health, *An Achievable Vision*, 15.

[70] Task Force on Mental Health, *An Achievable Vision*, exec. sum, 3. Soldiers' deep-seated wariness about seeking mental health assistance stems from certain norms or underlying assumptions held by military members (and, for that matter, society at large). One way to conceptualize the underlying beliefs that create stigma is to look at the soldier attitudes toward mental health services. In 2009, the Army's Mental Health Advisory Team asked deployed soldiers whether the following factors would affect their decision to receive mental health services: it would be too embarrassing; it would harm my career; members of my unit might have less confidence in me; my unit leadership might treat me differently; my leaders would blame me for the problem; I would be seen as weak. Positive responses to the individual questions ranged from 25 to 50 per cent of soldiers surveyed. Office of the Command Surgeon, US Forces Afghanistan (USFOR-A) and Office of The Surgeon General, United States Army Medical Command, *Mental Health Advisory Team (MHAT) 6, Operation Enduring Freedom 2009 Afghanistan* (Washington DC: U.S. Department of the Army, November 9, 2009), 35.

[71] General Chiarelli's reaction to a stigmatizing event disclosed online strongly demonstrated his resolve in this area. On Tuesday, May 11, 2009, Elspeth Reese revealed, in a story on the online "Daily Beast," that some commanders were requiring soldiers attending mental health counseling to wear yellow road guard vests. Elspeth Reeves, Suicidal Soldiers, May 11, 2009, http://www.thedailybeast.com/blogs-and-stories/2009-05-11/suicidal-soldiers/ (last accessed October 18, 2010). The "powerful stigma" of such a technique was obvious. On May 14, 2009, General Chiarelli responded firmly to combat such practices. He prohibited physical identification of soldiers seeking behavioral health services. He made clear that the way a leader treats soldiers obtaining mental health services is a "part of the leader's overall management of command climate and unit morale" that could be reflected in a leader's rating. Vice Chief of Staff of the Army Peter Chiarelli, "Commander and Leader Responsibilities – Removing Stigma," memorandum for all Army activities, Washington, DC, May 14, 2009.

[72] For example, as reported on www.army.mil, when General Chiarelli spoke to the US Army War College, he focused on the "'signature injuries' of the [Iraq and Afghanistan Wars], post-traumatic stress and traumatic brain injuries." Thomas Zimmerman, "Army leadership discusses today's issues with Army War College students," Oct 14, 2010, http://www.army.mil/-news/2010/10/14/46583-army-leadership-discusses-todays-issues-with-army-war-college-students/index.html (accessed October 18, 2010). General Chiarelli specifically stated, "[w]e

must remove the stigmas associated with getting help." Ibid. General Chiarelli frequently discusses stigma in the context of soldier behavioral health. For example, see, David Gura, "Army Vice Chief Peter Chiarelli Addresses Soldier Suicides, Drug Abuse," July 29, 2010 http://www.scpr.org/news/2010/07/29/army-vice-chief-peter-chiarelli-addresses-soldier-/ (discussing stigma and the Army's behavioral health report on NPR) (accessed October 18, 2010); Heather Graham-Ashley, "Vice chief: Army needs to address PTS, TBIs," September 23, 2010, http://www.army.mil/-news/2010/09/23/45556-vice-chief-army-needs-to-address-pts-tbis/, ("The first step, Chiarelli said, is in helping to eliminate the stigmas about behavioral health and treatment.") (accessed October 18, 2010); Matthew Cox, "Chiarelli: Reduce brain-injury stigma," October 6, 2009, http://www.armytimes.com/news/2009/10/army_vice_chief_100509w/ (accessed October 18, 2010).

[73] General Chiarelli wrote a "Vice Chief of Staff of the Army Sends" as the introduction to the Army Health Promotion, Risk Reduction, and Suicide Prevention Report. Army HP/RR/SP Report, i-iii. General Chiarelli spoke for a full hour at the Army Leader Forum concerning PTS and TBI. The final point on his last substantive slide read: "Be involved ... need <u>you</u> to help eliminate the stigma." Peter Chiarelli, lecture to Army Leader Forum, September 8, 2010. Video and presentation at http://www.army.mil/-news/2010/09/14/45170-army-leader-forum/index.html (last accessed October 18, 2010).

[74] The Army's recent report, Health Promotion, Risk Reduction, and Suicide Prevention (HP/RR/SP Report), similarly recommends that commanders "Ensure leaders at all levels encourage help-seeking behavior and convey anti-stigma messages as a routine matter of unit operations." Army HP/RR/SP Report, 23.

[75] Until March 2010, the Standard Questionnaire required to obtain a security clearance asked an applicant whether, "In the last 7 years, [you have] consulted with a mental health professional (psychiatrist, psychologist, counselor, etc.) or ... with another healthcare provider about a mental health related condition?" Office of Personnel Management, *Standard Form 86, Standard Questionnaire for National Security Positions* (Washington DC: U.S. Office of Personnel Management, September 1995).

[76] Office of Personnel Management, *Standard Form 86, Standard Questionnaire for National Security Positions* (Washington DC: U.S. Office of Personnel Management, June 2008).

[77] A security clearance is required for selection for certain jobs and MOSs. Loss of a security clearance would exclude service members from certain positions and would have an adverse impact on promotion. Therefore, by excluding PTS or TBI-related counseling from the security clearance calculus, DOD recognized the real and perceived importance of confidentiality or privacy of certain health information.

Other DOD level initiatives include: The Department of Defense's Mental Health Task Force (MHTF) recommended that DOD implement an "anti-stigma public education campaign." Task Force on Mental Health, *An Achievable Vision*, 16. Recommendations included, developing and implementing DOD-wide "core curricula on psychological health as an integral part of all levels of leadership training," training family members, and training medical personnel. Ibid., 18-20.

[78] Joe Gould, "Video shrinks distance to mental healthcare," June 14, 2010, http://www.armytimes.com/news/2010/06/army_video_mental_health_061310w/ (accessed October 18, 2010).

[79] C. Todd Lopez, "Pilot program allows Soldier self-referral for alcohol treatment," August 20, 2009, at http://www.army.mil/-news/2009/08/20/26350-pilot-program-allows-soldier-self-referral-for-alcohol-treatment/ (accessed March 12, 2011).

[80] For example, counseling sessions take place outside of duty hours. Lopez, "Pilot Program."

[81] Gibbs and Olmstead, "Confidential Alcohol Treatment and Education Program," 109. The pilot program provided "a means for Soldier reparation and return to readiness, while enhancing the Army's anti-stigma objectives." Army HP/RR/SP Report, 63.

[82] Gibbs and Olmstead, "Confidential Alcohol Treatment and Education Program," 107-110.

[83] Military OneSource is an on-line or telephone resource available to military members, spouses and families. Military OneSource is designed to provide "help … with just about any need." Services include "[e]ducation, relocation, parenting, [and] stress." Military OneSource offers face-to-face, online and phone counseling. "The service is completely private and confidential, with few exceptions." *Military OneSource About Page*, http://www.militaryonesource.com/MOS/About.aspx (accessed March 21, 2011).

[84] *Military OneSource Counseling Options Page*, http://www.militaryOneSource.com/MOS/About/CounselingServices.aspx (accessed March 12, 2011).

[85] *Military OneSource Privacy/Reportable Issues FAQs,* http://www.militaryonesource.com/MOS/About/FAQs/tabid/198/uc/main/parentID/10/Default.aspx (accessed March 12, 2011).

The Army and DOD have initiated additional stigma-reducing efforts. The HP/RR/SP Report indicated that the Army was now requiring all soldiers to in and out process through Behavioral Health, Social Work Services and ASAP. According to the report, this new requirement has already "reduced the stigma associated with counseling services." Army HP/RR/SP Report, 127. In addition, the HR/RR/SP Report's recommended that commanders direct "all unit members receive BH screening after stressful events, as a means to reduce stigma." Army HP/RR/SP Report, 154.

The Mental Health Task Force recommended a number of structural changes to the provision of mental healthcare that would reduce stigma of seeking such services. For example, the MHTF recommended "embedding uniformed providers in military units." Task Force on Mental Health, *An Achievable Vision*, 17. The Mental Health Task Force also recommended "integrating mental health professionals into primary care settings." Task Force on Mental Health, *An Achievable Vision*, 18.

[86] Daniel Solove, A Brief History of Information Privacy Law in Kristin J. Mathews, ed., *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age* (Practising Law Institute, February 2011), 17.

[87] Ibid., citing, McCormick v. England, 494 S.E.2d 431 (S.C. Ct. App. 1997).

[88] 429 U.S. 589, 599-600 (1977) (upholding a New York law that permitted the collection of names and addresses of persons prescribed dangerous drugs. The Court found that the statute's "security provisions," adequately protected against "public disclosure" of patient information, and thereby protected a privacy interest "arguably ... root[ed] in the Constitution," 429 U.S. at 605). The Court reiterated the existence of such a right in *Nixon v. Admin of Gen'l*

Services also in 1977. Nixon v. Admin of Gen'l Services, 433 U.S. 425 (1977) (finding that government officials, including the President, do not wholly give up their constitutional privacy rights in matters of personal life unrelated to acts done in their public capacity).

[89] National Aeronautics and Space Admin. v. Nelson, 131 S.Ct. 746 (2011), decided January 19, 2011. Federal contractor employees challenged mandatory background check questions about treatment or counseling for recent illegal-drug use and certain open-ended questions sent to employees' references. The Court held the challenged portions of the Government's background check do not violate this right in the present case. "The Government's interests as employer and proprietor in managing its internal operations, combined with the protections against public dissemination provided by the Privacy Act of 1974, 5 U.S.C. § 552a, satisfy any 'interest in avoiding disclosure' that may 'arguably ha[ve] its roots in the Constitution.'" Ibid., 751.

[90] For example the appellate brief for the respondents in National Aeronautics and Space Admin. v. Nelson, provides:

> a broad consensus has developed in the lower courts as to both the scope of the right and the level of scrutiny required: the right protects sensitive personal information, including medical information, personal financial information and information about private sexual matters; and informational privacy claims merit heightened scrutiny.

Appellate Brief, National Aeronautics and Space Admin. v. Nelson, 2010 Westlaw 3048324 (August 2, 2010), 12. In addition,

> On the scope of the right, there is broad agreement in the federal circuit courts that the constitutional right to informational privacy protects sensitive personal information, including medical information ... There is also broad consensus that informational privacy claims merit heightened scrutiny. This process calls for the "delicate task of weighing competing interests." … Thus, "courts balance the government's interest in having or using the information against the individual's interest in denying access." ... The government must establish that its interest in obtaining or disclosing the information is sufficiently weighty to justify the intrusion into that personal sphere. The government must also establish that its use of the information will actually further that purpose, such that its intrusion into the personal sphere does not reach beyond the scope necessary to accomplish its legitimate interests.

Ibid., 18-19 (internal footnotes omitted).

[91] *Health Insurance Portability And Accountability Act,* Public Law 191, 104th Congress, 2nd sess. (August 2, 1996).

[92] Interestingly, privacy/confidentiality rules were not initially part of the Act. Instead, Congress directed the Department of Health and Human Services (HHS) to provide a recommended regulatory scheme. The Act provided that HHS regulations could be promulgated as binding rules should Congress not pass privacy provisions within three years of HIPAA passage. Congress failed to pass privacy rules. On November 3, 1999, HHS published draft privacy rules. HHS received over 52,000 comments on the proposed rules. HHS published final rules on December 28, 2000. Modified rules, published on August 14, 2002 are still in effect today. Department of Health and Human Services, Office of Civil Rights, *Summary*

of the HIPAA Privacy Rule, (Washington, DC: Department of Health and Human Services, May, 2003), 2.

[93] HHS OCR, *Summary*, 1. "A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality healthcare and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing." Ibid.

[94] Ibid., 4.

[95] Ibid., 2.

[96] U.S. Department of Defense, Assistant Secretary of Defense for Health Affairs, *DOD Health Information Privacy Regulation,* U.S. Department of Defense Regulation 6025.18-R (Washington, DC: U.S. Department of Defense, January 2003), 35.

[97] HHS OCR, *Summary*, 3-4.

[98] Ibid., 4.

[99] Ibid., 4-5, providing: "A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or healthcare operations."

[100] Ibid., 5.

[101] 45 Code of Federal Regulations Section 164.506(c). (hereafter, 45 CFR)

[102] 45 CFR § 164.512.

[103] HHS OCR, *Summary*, 6.

[104] 45 C.F.R. § 164.512 (a).

[105] 45 C.F.R. § 164.512 (b).

[106] 45 C.F.R. § 164.512 (a) and (c).

[107] 45 C.F.R. § 164.512 (d).

[108] 45 C.F.R. § 164.512 (e).

[109] 45 C.F.R. § 164.512 (f).

[110] 45 C.F.R. § 164.512(j). See also, HHS OCR, *Summary*, 8:
Covered entities may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the

public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.

[111] 45 C.F.R. § 164.512(k). Among these government functions is the proper execution of a military mission.

[112] 45 C.F.R. § 164.508(a)(2).

[113] HHS OCR, *Summary*, 10.

[114] HHS OCR, *Summary*, 10. See also, 45 CFR § 164.502(b) and § 164.514(d).

[115] 45 C.F.R. § 164.512(k). The military disclosure provision states:

A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the FEDERAL REGISTER the following information: (A) Appropriate military command authorities; and (B) The purposes for which the protected health information may be used or disclosed.

[116] U.S. Department of Defense, Assistant Secretary of Defense for Health Affairs, *DOD Health Information Privacy Regulation,* U.S. Department of Defense Regulation 6025.18-R (Washington, DC: U.S. Department of Defense, January 2003). Because the regulation governs treatment of both service members and family members, the disclosure rules in DOD 6025-18-R pertaining to non-military patients, substantially mirror HIPAA's Privacy Rule regulations. Ibid., 24-35. In fact, the "Rules and Procedures established by the Secretary of HHS ... are applicable" to DOD covered entities. Ibid., 31. Complaints of violations are filed with HHS. Ibid.

[117] The regulation defined the "appropriate military command authorities" who may designate those activities necessary to assure proper execution of the military mission, thus triggering when a covered entity may use and disclose the protected health information of Armed Forces personnel. Ibid., 69. Those authorities are: "All Commanders who exercise authority over a" service member "or other person designated by such a commander"; "The Secretary of Defense, the Secretary of the Military Department"; and, "Any official delegated authority by a Secretary ... to take an action designed to ensure the proper execution of the military mission." Ibid.

[118] Department of Defense, *Health Information Privacy Regulation,* 69-70. DOD published the required notice in the Federal Register in April, 2003. U.S. Department of Defense Notice: Health Information Privacy, 68 Federal Register 17357-02 (April 9, 2003). ("Provisions are made to allow appropriate uses and disclosures of protected health information concerning members of the armed forces to assure the proper execution of the military mission, provided that the Department of Defense publishes in the Federal Register a notice describing implementation of these provisions. This notice implements those provisions.") No further notices have been

published in the Federal Register concerning disclosure of service member PHI. The author conducted a search on Westlaw on January 16, 2011.

[119] Gail McGinn, Deputy Under Secretary of Defense (Plans), Performing the Duties of Under Secretary of Defense (Personnel and Readiness), "Revising Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Military Personnel," Directive-Type Memorandum (DTM) 09-006 for Secretaries of the Military Departments, et. al., Washington, DC, July 2, 2009.

[120] McGinn, Requirements to Dispel Stigma, 1.

[121] McGinn, Requirements to Dispel Stigma, 2.

[122] The author conducted various searches on Google as well as Westlaw (searching various case law, statute and regulation databases).

[123] McGinn, Requirements to Dispel Stigma, attachment 2. The DTM reiterated DOD policy that when circumstances required disclosure of PHI, the "minimum amount of information" shall be provided. The directive described the information that generally should be disclosed: the diagnosis, a description of the intended treatment, the impact on the mission, recommended duty restrictions and the prognosis. Ibid., 2.

[124] U.S. Department of the Army, *Rapid Action Revision Medical Record Administration and Healthcare Documentation,* Army Regulation 40-66 (Washington, DC: U.S. Department of the Army, January 10, 2010), 1.

[125] Ibid.,2.

[126] Ibid., 7. These included: to "coordinate sick call, routine and emergency care, quarters, hospitalization, and care from civilian providers"; to "report results of physical examinations and profiling"; to "screen and provide periodic updates for individuals in special programs" ; "to review and report according to" the Army Weight Control Program"; "to initiate line of duty (LOD) determinations and to assist" LOD investigating officers; "to conduct medical evaluation boards and administer physical evaluation board findings"; to "review and report according to" the Human Immunodeficiency Virus (HIV) program; to "carry out activities under the authority of" the preventive medicine program "to safeguard the health of the military community"; to "report on casualties in any military operation or activity"; to "medically administer flying restrictions"; to "participate in aircraft accident investigations"; to "respond to queries of accident investigation officers to complete accident reporting"; to "report mental status evaluations"; to "report special interest patients according to AR 40-400" ; to "report the Soldier's dental classification"; to "carry out Soldier Readiness Program and mobilization processing requirements"; to "provide initial and follow-up reports according to" the Army Family Advocacy Program; to "contribute to the completion of records according to" the Exceptional Family Member Program; to "allow senior commanders to review Soldier medical information to determine eligibility of assignment/ attachment to a warrior transition unit (WTU)."; and, "[a]ccording to other regulations carrying out any other activity necessary to the proper execution of the Army's mission." Ibid.

[127] Ibid. The RAR also identifies three additional permitted disclosures of PHI under limited circumstances. Absent objection, limited information may be included in a military treatment facility directory, Ibid., 6; absent objection, disclosures may be made to a family member, other

relative or a close personal friend, Ibid., 6-7; disclosures may be made to assist in disaster relief, Ibid., 7.

[128] Ibid., 8 ("For example, a Soldier indicates that he is thinking of hurting himself or his wife, or a Soldier is determined to be ill enough to be in need of psychiatric hospitalization.")

[129] Ibid. ("For example, a Soldier is receiving care for behavioral health issues, family advocacy, and for substance abuse. Note. Routine behavioral healthcare would not trigger command notification.")

[130] Ibid. ("For example, a Soldier is placed on lithium which can reach toxic levels if the Soldier is dehydrated, or a Soldier is prescribed a pain medication that alters expected sleep pattern. Note. A Soldier on lithium cannot deploy.")

[131] Ibid. ("For example, a Soldier becomes delusional or has hallucinations, or a Soldier develops epilepsy.")

[132] Ibid. The regulation also provides procedural guidance for the disclosure of PHI and delineates specific accounting requirements and reiterates the requirement to only provide the "minimum necessary information." Ibid.

[133] Vice Chief of Staff of the Army Pete Chiarelli, "VCSA Sends On Protected Health Information (PHI)," Memorandum for All Army Activities (ALARACT), Washington, DC, May 28, 2010.

[134] Ibid.

[135] Ibid.

[136] Ibid.

[137] Ibid.

[138] Ibid.

[139] Ibid.

[140] Ibid.

[141] Ibid.

[142] Herbert S. Coley, Chief of Staff, for the Commander, U.S. Department of the Army Office of the Surgeon General and Medical Command, "OTSG/MEDCOM Policy Memo 10-042, Release of Protected Health Information to Unit Command Officials," Memorandum for Commanders, MEDCOM Major Subordinate Commands, Washington, D.C., June 30, 2010.

[143] Ibid.

[144] 10-042 also captures other regulatory guidance regarding disclosure previously discussed in this paper. It sets forth five circumstances in which the minimum necessary disclosure of PHI may be made absent soldier authorization: to determine the members fitness

for duty; to determine the members fitness to perform any particular mission; to carry out Joint Medical Surveillance activities; to report casualties; "to carry out any other activity necessary to the proper execution of the mission of the Armed forces." It lays out 22 examples of "regulatory and command management programs that do not require a Soldier's authorization for PHI disclosure." Ibid. These areas substantially overlap those captured in Army Regulation 40-66 and discussed above.

[145] Department of Defense, *Health Information Privacy Regulation*, 23 and 33.

[146] Department of the Army, *Medical Record Administration and Healthcare Documentation,* 4. Therefore, medical information covered by both regulations may be disclosed outside of the federal government only if disclosure is authorized by both regulations. U.S. Department of Defense, *Department of Defense Privacy Program*, Department of Defense Regulation 5400-11R, (Washington, DC: U.S. Department of Defense, May 14, 2007), 47.

[147] Typically, personal records are withheld when disclosure would "result in a clearly unwarranted invasion of the individual's personal privacy." Department of Defense, *DOD Privacy Program*, 38, referencing the Defense Department's implementation of the Freedom of Information Act in U.S. Department of Defense, *Department of Defense Freedom of Information Act Program*, Department of Defense Regulation 5400-7R, (Washington, DC: U.S. Department of Defense, September 1, 1998), 37.

[148] Department of Defense, *DOD Privacy Program*, 38. All of DOD is considered a single agency for purposes of the Privacy Act. Ibid., 37. Within DOD, "Records pertaining to an individual may be disclosed to a DOD official or employee provided: ... The requester has a need for the record in the performance of his or her assigned duties." Ibid., 38.

[149] Vice Chief of Staff of the Army Pete Chiarelli, "VCSA Sends On Protected Health Information (PHI)," Memorandum for All Army Activities (ALARACT), Washington, DC, May 28, 2010.

[150] Ibid.

[151] Ibid.

[152] U.S. Department of the Army, *Army Leadership*, Army Regulation 600-100 (Washington, DC: U.S. Department of the Army, March 8, 2007), 1.

[153] U.S. Department of Defense, Under Secretary of Defense (Personnel and Readiness), SD(P&R), *Counseling Services for Department of Defense Military, Guard and Reserve, Certain Affiliated Personnel, and Their Family Members* (Washington, DC: Department of Defense, April 21, 2009) 1.

[154] Howe, "Mixed Agency in Military Medicine, 344.

[155] AMA Ethics Opinion 5.05.

[156] U.S. Department of the Army, *Army Leadership*, Army Regulation 600-100 (Washington, DC: U.S. Department of the Army, March 8, 2007), 1. See also, U.S. Department of the Army *2010 Army Posture Statement*, (Washington, DC: U.S. Department of the Army, February

2010), 7 (“Sustaining our all-volunteer force is our first imperative.... The Army is committed to ensuring that the quality of life of those who serve the Nation is commensurate with the quality of their service.”).